

CLAIMS

What is claimed is:

- 1 1. A computerized method for scanning files for viruses comprising:
2 generating a current session key upon an execution of the method;
3 obtaining a session stamp associated with a directory entry for a file;
4 scanning the file if the session stamp was created using a previous session key; and
5 updating the session stamp as a result of the scan.
- 1 2. The method of claim 1, further comprising:
2 scanning the file if there is no session stamp associated with the directory entry for
3 the file; and
4 creating a session stamp using the current session key as a result of the scan.
- 1 3. The method of claim 1, wherein updating the session stamp comprises invalidating
2 the session stamp if the file is infected with a virus.
- 1 4. The method of claim 1, wherein the session stamp comprises an infection indicator
2 and updating the session stamp comprises modifying the infection indicator when the file is
3 infected with a virus.
- 1 5. The method of claim 1, wherein the session stamp comprises a signature and
2 updating the session stamp comprises encrypting a known value with the current session
3 key to create the signature.

1 6. The method of claim 1, wherein the session stamp comprises a signature and
2 updating the session stamp comprises replacing a previous session key with the current
3 session key.

1 7. The method of claim 1, wherein the session stamp comprises context information
2 and updating the session stamp comprises replacing previous context information with
3 current context information.

1 8. The method of claim 1, wherein obtaining the session stamp, scanning the file, and
2 updating the session stamp are performed when the file is accessed.

1 9. The method of claim 1, wherein obtaining the session stamp, scanning the file, and
2 updating the session stamp are performed upon the file as a result of a user command.

1 10. The method of claim 1, further comprising:
2 loading a pre-determined set of file identifiers, wherein obtaining the session
3 stamp, scanning the file, and updating the session stamp are performed on each file
4 identified by the file identifiers.

1 11. The method of claim 10, wherein the pre-determined set of file identifiers is a
2 most-recently-used cache of identifiers for the files that have been most recently used, and
3 further comprising:

4 adding an identifier for the file to the most-recently-used cache when the file is
5 accessed; and

6 storing the most-recently-used cache to non-volatile storage upon termination of
7 the execution.

1 12. The method of claim 10, wherein the pre-determined set of file identifiers is
2 created from user input.

a! 1 13. The method of claim 10, wherein obtaining the session stamp, scanning the file,
2 and updating the session stamp are performed as a background task on each file identified
3 by the file identifiers.

1 14. The method of claim 1, wherein the session stamp is stored in an extended
2 attributes section of the directory entry for the file.

001 1 15. A computer-readable medium having stored thereon executable instructions to
2 cause a computer to perform a method comprising:
3 generating a current session key upon an execution of the instructions;
4 obtaining a session stamp associated with a directory entry for a file;
5 scanning the file if the session stamp was created using a previous session key; and
6 updating the session stamp as a result of the scan.

1 16. The computer-readable medium of claim 15, further comprising:
1 scanning the file if there is no session stamp associated with the directory entry for
2 the file; and
3 creating a session stamp using the current session key as a result of the scan.

1 17. The computer-readable medium of claim 15, wherein obtaining the session stamp,
2 scanning the file, and updating the session stamp are performed when the file is accessed.

a

00114-09073760

1 18. The computer-readable medium of claim 15, wherein obtaining the session stamp,
2 scanning the file, and updating the session stamp are performed upon the file as a result of
3 a user command.

1 19. The computer-readable medium of claim 15, further comprising:
2 loading a pre-determined set of file identifiers, wherein obtaining the session
3 stamp, scanning the file, and updating the session stamp are performed on each file
4 identified by the file identifier.

1 20. The computer-readable medium of claim 15, wherein the session stamp is stored in
2 an extended attributes section of the directory entry for the file.

1 21. A computer-readable medium having stored thereon a session stamp data structure
2 comprising:
3 a file identifier field containing data representing an identifier for a file in a file
4 system; and
5 a signature field containing data created by an execution of an anti-virus process
6 that last scanned the file identified by the file identifier field.

1 22. The computer-readable medium of claim 21, wherein the data in the signature field
2 represents a pre-determined value encrypted by a session key associated with the
3 execution of the anti-virus process.

1 23. The computer-readable medium of claim 21, wherein the data in the signature field
2 represents a session key associated with the execution of the anti-virus process.

1 24. The computer-readable medium of claim 21, further comprising:
2 a scanner settings field containing data representing a configuration for the anti-
3 virus process that last scanned the file identified by the file identifier field.

1 25. The computer-readable medium of claim 21, further comprising:
2 a scan result field containing data representing an infection status returned by the
3 anti-virus process that last scanned the file identified by the file identifier field.

1 26. The computer readable medium of claim 21, further comprising:
2 a time and date stamp field containing data representing a time and date the file
3 identified by the file identifier field was last modified.

1 27. The computer-readable medium of claim 21, further comprising:
2 a size field containing data representing a size for the file identified by the file
3 identifier field.

1 28. A computer system comprising:
2 a processor coupled to a system bus;
3 a memory coupled to the processor through the system bus;
4 a computer-readable medium coupled to the processor through the system bus;
5 a virus scanning process executed from the computer-readable medium by the
6 processor, wherein the scanning process causes the processor to generate a current session
7 key when the scanning process is executed from the computer-readable medium, and
8 further to obtain a session stamp associated with a directory entry for a file from the
9 computer-readable medium, to scan the file if the session stamp was created using a

a1

00114.P007

10 previous session key, and to update the session stamp on the computer-readable medium
11 as a result of the scan.

1 29. The computer system of claim 28, wherein the virus scanning process further
2 causes the processor to scan the file if there is no session stamp associated with the
3 directory entry for the file on the computer-readable medium, to create a session stamp
4 using the current session key as a result of the scan, and to store the session stamp in the
5 directory entry for the file on the computer-readable medium.

1 30. The computer system of claim 28, further comprising a user input device coupled
2 to the processor through the system bus, wherein input from the user input device
3 instructs the virus scanning process to scan the file.

1 31. The computer system of claim 28, further comprising an application process
2 executed from the computer-readable medium by the process, wherein a request from the
3 application process for the file causes the processor to scan the file.

1 32. A method for communicating between an anti-virus process and a session stamping
2 process comprising:

3 issuing, by the anti-virus process, an enable-session-key call;

4 receiving, by the session stamping process, the enable-session-key call and, in
5 response thereto, initializing a stamping session and generating a session key;

6 issuing, by the anti-virus process, a disable-session-key call; and

7 receiving, by the session stamping process, the disable-session-key call and, in
8 response thereto, disabling the stamping session.

1 33. The method of claim 32, further comprising:
2 issuing, by the anti-virus process, a stamp-file-with-session-stamp call having a file
3 parameter; and
4 receiving, by the session stamping process, the stamp-file-with-session-stamp call
5 and, in response thereto, generating a session stamp using the session key and associating
6 the session stamp with a file identified by the file parameter.

1 34. The method of claim 33, wherein the stamp-file-with-session-stamp call further has
2 an engine parameter identifying context information used to generate the session stamp.

1 35. The method of claim 33, wherein the stamp-file-with-session-stamp call further has
2 an iam parameter identifying the anti-virus process currently calling the session stamping
3 process.

1 36. The method of claim 32, further comprising:
2 issuing, by the anti-virus process, a delete-session-stamp call having a file
3 parameter; and
4 receiving, by the session stamping process, the delete-session-stamp call and, in
5 response thereto, deleting any session stamp associated with the file identified by the file
6 parameter.

1 37. The method of claim 32, further comprising:
2 issuing, by the anti-virus process, a has-file-got-valid-session-stamp call having a
3 file parameter;

4 receiving, by the session stamping process, the has-file-got-valid-session-stamp call
5 and, in response thereto, determining a validity for any session stamp associated with the
6 file identified by the file parameter; and
7 returning, by the session stamping process, the validity to the anti-virus process.

a 1 38. The method of claim 37, wherein the has-file-got-valid-session-stamp call further
2 has an engine parameter identifying context information used to determine the validity of
3 the session stamp.

1 39. The method of claim 37, wherein the has-file-got-valid-session-stamp call further
2 has an iam parameter identifying the anti-virus process currently calling the session
3 stamping process.

1 40. The method of claim 37, wherein the has-file-got-valid-session-stamp call further
2 has a signer parameter, and further comprising:
3 returning, by the session stamping process, an identifier for the anti-virus process
4 that last called the session stamping process as the signer parameter.